LLM MultiChat

Security Report

Erstellt: 18.12.2025

WICHTIGER HINWEIS: Diese Software wurde zu 100% von kuenstlicher Intelligenz (Claude, Anthropic) generiert. Es wurde keine manuelle Codepruefung durchgefuehrt. Die Nutzung erfolgt auf eigene Gefahr und Verantwortung.

1. Zusammenfassung

LLM MultiChat ist eine Electron-basierte Desktop-Anwendung, die mehrere KI-Chat-Dienste (ChatGPT, Claude, Copilot, Gemini, etc.) in einer einheitlichen Oberflaeche zusammenfasst. Die Anwendung wurde vollstaendig durch KI-gestuetzte Codegenerierung erstellt.

2. Technische Architektur

Verwendete Technologien:

Komponente	Technologie	Version
Runtime	Electron	~28.0.0
Backend	Node.js	20.x LTS
Frontend	HTML/CSS/JavaScript	ES6+
Webviews	Chromium (via Electron)	entsprechend Electron

3. Sicherheitsanalyse

3.1 Webview-Isolation

Die Anwendung verwendet Electron Webviews mit aktivierter Context-Isolation und deaktiviertem Node-Integration. Jeder KI-Dienst laeuft in einem separaten Webview-Prozess.

3.2 Preload-Script

Das Preload-Script exponiert nur eine minimale API (contextBridge) fuer die Kommunikation zwischen Renderer und Main-Prozess. Folgende IPC-Kanaele sind definiert:

- copy-to-clipboard: Kopiert Text in die Zwischenablage

3.3 Netzwerkkommunikation

Die Anwendung kommuniziert ausschliesslich mit den offiziellen Webseiten der KI-Dienste. Update-Pruefungen erfolgen ueber die GitHub API (api.github.com).

4. Identifizierte Risiken

Risiko	Schweregrad	Beschreibung
KI-generierter Code	Mittel	Code wurde nicht manuell geprueft
Webview-Sicherheit	Niedrig	Abhaengig von Chromium-Updates
Update-Mechanismus	Niedrig	Downloads von GitHub ohne Signatur
Lokale Datenspeicherung	Niedrig	Configs im Klartext

5. Empfehlungen

- Verwenden Sie die Software nicht fuer sensible oder vertrauliche Daten
- Halten Sie Electron und Node.js auf dem neuesten Stand
- Pruefen Sie regelmaessig auf Updates
- Verwenden Sie die Software nur in vertrauenswuerdigen Netzwerken
- Bei Sicherheitsbedenken: Quellcode auf GitHub einsehen

6. Haftungsausschluss

Diese Software wird "wie besehen" (as-is) bereitgestellt, ohne jegliche ausdrueckliche oder stillschweigende Garantie. Der Autor uebernimmt keine Haftung fuer Schaeden, die durch die Nutzung dieser Software entstehen koennten.

Der gesamte Quellcode wurde von KI-Systemen generiert und nicht von Menschen geprueft. Die Nutzung erfolgt ausschliesslich auf eigene Gefahr und Verantwortung des Anwenders.

7. Quellcode und Transparenz

Der vollstaendige Quellcode ist oeffentlich einsehbar unter:

https://github.com/3Dcut/multiLLM

Issues und Sicherheitsmeldungen koennen dort gemeldet werden.